**IT Applications, Ch 7, Information Management**

Threats to the integrity and security of data and information stored, communicated and disposed of by organisations.

Complete the following from p 270

**Deliberate threats**

1. When does intentional damage occur?
2. Unauthorised access is both physical and logical. Explain what this means?
3. Computer Virus
   1. Describe the nature of this virus.
      * A computer virus infects a machine in much the same manner as a biological virus might infect a human, is one of the most common and easily transmitted threats to data stored in computers
   2. What is the main purpose of a virus?
      * The main purpose of a virus is to affect the running of the PC in a manner unintended by its user.
   3. What is meant by the term, payload?
      * Payload is the action that the virus is designed to carry out, such as deleting files from the hard disk or randomly sending email to recipients found in the address book.
   4. Describe a worm?
      * A worm is a virus that self-replicates to take up space on a hard disk on a single workstation or server.
   5. List the other types of viruses, p 272, fig. 7-10.
      * Boot infectors
      * Executable
      * Macro
      * Time bomb
      * Logic bomb
      * Trojan horse
      * Resident
      * Polymorphic
   6. How do viruses mainly spread?
      * There are several ways that viruses can spread but the most common is through an email file attachment, or by the transfer of infected files on removable storage devices. Another less common way is by different users accessing an infected file on a network.
4. Hacking/Cracking
   1. Who is a hacker and what damage do they cause?
      * A hacker is a person who gains unauthorised access to an information system through logical means in order to look at the stored data or simply for the challenge. Hackers are most commonly associated with breaking into information systems and looking at any interesting or confidential material that they may contain.
5. Tampering with files
   1. Describe how employees tamper with files.
      * Employees have tampered with salary amounts and even erased important medical files from hospital databases of patient details.
   2. What is industrial sabotage?
      * Industrial sabotage can appeal to countries that are attractive to inverters but have poor finances of their own. Companies investing in these countries may find that the transmission of electronic communications is controlled by a corrupt government that threatens to deny access to the communication systems unless they pay large sums of money.
6. Information theft
   1. Why does this occur?
      * Information theft can occur for organisations to get an edge over their competitors.
7. Vandalism of hardware
   * + Some hardware breakage can be caused by acts of vandalism, people will deliberately damage equipment. Vandalism creates added expenses due to costs to repair the object.
8. Theft of hardware
   * + With computer hardware in great demand, it is not surprising that theft is a problem. Due to the size of desktop computers they are usually too hard to steal so thieves try and steal smaller things such as RAM chips and hard disks.

**Accidental threats**

1. User error
   1. List some common examples of user error.
   * Unaware of how to operate equipment properly
   * Copyright an older version of a file over a newer version or formatting a disk that contains important data
   1. What processes are in place to limit user error.
   * Building safeguards such as dialogue boxes to confirm particular actions
2. Failure to follow file-management procedures
   1. List common errors of employees in saving files.
   * File extensions have been left off
   * Non-descriptive filenames were used
   * Folders were improperly used

**Technical Failure**

1. List some examples of technical failure.
   * Graphic cards stop working
   * Hard disks fail
   * Operating system not working properly

**Consequences of violating security and privacy measures, p 278**

1. List three important consequences if security measures are violated.
   * Breaches of privacy
   * Loss of intellectual property
   * Loss of income due to unavailability of information or services